(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 172 731 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
01.09.2004 Bulletin 2004/36

(51) Int Cl.[7]: **G06F 12/14**

(21) Application number: **00311444.4**

(22) Date of filing: **20.12.2000**

(54) **Data processing apparatus and integrated circuit**

Datenverarbeitungsgerät und Integrierte Schaltung

Appareil de traitement de données et circuit intégré

(84) Designated Contracting States:
DE FR GB

(30) Priority: **13.07.2000 JP 2000212815**

(43) Date of publication of application:
16.01.2002 Bulletin 2002/03

(73) Proprietor: **FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211-8588 (JP)

(72) Inventors:
- **Kawasaki, Yusuke, Fujitsu Limited**
  Kawasaki-shi, Kanagawa 211-8588 (JP)
- **Sakurai, Hiroshi, c/o Fujitsu Limited**
  Kawasaki-shi, Kanagawa 211-8588 (JP)
- **Hashimoto, Shigeru, c/o Fujitsu Limited**
  Kawasaki-shi, Kanagawa 211-8588 (JP)
- **Yamamoto, Koken, c/o Fujitsu Limited**
  Kawasaki-shi, Kanagawa 211-8588 (JP)

(74) Representative: **Fenlon, Christine Lesley et al**
Haseltine Lake & Co.,
Imperial House,
15-19 Kingsway
London WC2B 6UD (GB)

(56) References cited:
EP-A- 0 660 215
EP-A- 0 720 098
EP-A- 1 093 056
WO-A-00/19321
WO-A-99/13615
DE-A- 19 922 155
FR-A- 2 787 216
US-A- 4 573 119
US-A- 5 081 675
US-A- 5 488 661
US-A- 5 515 540

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 1 172 731 B1

Description

[0001] The present invention relates to a processing apparatus comprising an internal circuit having a CPU and internal devices, and an external circuit including external devices provided externally of the internal circuit, and to an integrated circuit incorporating such processing apparatus.

[0002] With the recent development of LSI, a CPU executing programs, a memory storing the programs executed by the CPU and various other devices have been able to be integrated on one chip, which contributes greatly to making an apparatus small in size, achieving cost reduction and the like. To manufacture such LSI, it suffices to mount a memory storing programs on a LSI chip if a system executes the same programs irrespectively of users and does not need to change programs after completion. However, if it is necessary to execute different programs according to users or to change a program while the program is in use, it is desirable to constitute LSI so that an external memory can be further provided externally of the LSI having the above constitution and to store programs which may be possibly changed while in use or programs which differ according to users in the external memory.

[0003] Meanwhile, in case of a system capable of adding such an external memory externally of the LSI, however, there is a probability that the content of the external memory is illicitly rewritten or the external memory is replaced by a memory storing an illicit program and having the same specification as that of the external memory, with the result that important programs or data stored in the internal memory are illicitly accessed and the contents of the programs or data are illicitly interpreted. The following is one example of this case.

[0004] Recently, IC cards and magnetic cards each having a cash value or a point value corresponding to a cash as data is spreading increasingly. Following this, it is of urgent necessity to ensure data security so as to prevent the fabrication or falsification of cards. To this end, methods of preventing the reverse engineering of an apparatus were attempted in the past. Despite these attempts, it is the present situation that illicit ROMs and the like are created and apparatuses are incessantly abused against developers' will.

[0005] Accordingly, it is desirable to provide a processing apparatus and an integrated circuit intended to prevent illicit access and reverse engineering.

[0006] In this regard, EP-A-0720098 and US-A-5081675 disclose a processing apparatus comprising: an internal circuit including a CPU executing programs, at least one internal device having a predetermined function and bus line means connecting said CPU to said internal device, extending externally and transferring an address and data; and an external circuit provided externally of an externally extending portion of said bus line means and including at least one external device having a predetermined function, wherein said internal circuit includes a ciphering section interposed at an entrance to an external side and ciphering the address and the data on the bus line means by ciphering patterns according to a plurality of regions divided from an address space allotted to the entirety of said at least one external device.

[0007] US-A-5515540 and EP-A-1093056 are also of relevance to the problems addressed by the present invention.

[0008] According to a first aspect of the present invention there is provided a processing apparatus comprising:

> an internal circuit including a CPU executing programs, at least one internal device having a predetermined function and bus line means connecting said CPU to said internal device, extending externally and transferring an address and data; and an external circuit provided externally of an externally extending portion of said bus line means and including at least one external device having a predetermined function, wherein said internal circuit includes a ciphering section interposed at an entrance to an external side and ciphering the address and the data on the bus line means by ciphering patterns according to a plurality of regions divided from an address space allotted to the entirety of said at least one external device;

characterised in that said ciphering section outputs a dummy address and dummy data to the externally extending portion of said bus line means at timing at which said external circuit is not accessed.

[0009] Since the ciphering section outputs a dummy address and dummy data to the externally extending portion of the bus line at timing at which the external circuit is not accessed, illicit interpretation is made more difficult.

[0010] Here, the ciphering patterns adopted by the ciphering section include one ciphering pattern in which neither the address nor data is ciphered.

[0011] As stated above, by dividing the address space into a plurality of areas and ciphering the address and the data by the patterns which differ according to the divided areas, it is made difficult to interpret ciphers.

[0012] In the first processing apparatus embodying the present invention stated above, it is preferable that the external circuit includes a plurality of external devices; and

the ciphering section performs ciphering using ciphering patterns according to the plurality of external devices, respectively.

[0013] By doing so, it is possible to perform ciphering according to the property of the external device as follows. If a flash ROM is provided as one of the external devices, for example, both the address and the data are ciphered for the flash ROM. As for a RAM, as one of the external devices, which can read continuous addresses

at high speed, only the data is ciphered or the addresses are ciphered but the lower bit side of the addresses continuously read are not ciphered. If an I/O device is provided as one of the external devices, neither the address nor data is ciphered.

[0014] Furthermore, in the processing apparatus embodying the present invention stated above, it is preferable that the CPU is supplied with a clock and executes the programs synchronously with the supplied clock, and the ciphering section is supplied with a clock and performs ciphering synchronously with the supplied clock; and a clock supply section for supplying a clock at a higher speed than a speed of the clock supplied to the CPU, to the ciphering section.

[0015] This makes complicated ciphering possible.

[0016] Moreover, in the processing apparatus embodying the present invention, it is preferable that the processing apparatus comprises ciphering pattern determination means for recognizing a constitution of the external circuit and determining a ciphering pattern of the ciphering section according to the constitution of the external circuit.

[0017] By providing this ciphering pattern determination means, it becomes unnecessary to carry out operations such as the operator's determination of ciphering patterns according to different constitutions of the external circuit.

[0018] Further, in the processing apparatus embodying the present invention stated above, it is preferable that the ciphering section ciphers the address and the data on the bus line by ciphering patterns according to the plurality of regions divided from the address space allotted to the entirety of the no less than one external device and according to application programs executed by the CPU.

[0019] This makes ciphering patterns more complicated and illicit interpretation more difficult.

[0020] Furthermore, in the processing apparatus embodying the present invention stated above, it is preferable that a deciphering section connected to the externally extending portion of the bus line, and returning the ciphered address and the data on the bus line to an address and data which are not ciphered.

[0021] If debugging is to be performed without providing this deciphering section, the debugging becomes extremely difficult since the address and data are ciphered. Considering this, this deciphering section is provided, thereby making it possible to easily carry out debugging at the time of developing the processing apparatus.

[0022] This deciphering section becomes unnecessary after the completion of debugging. Therefore, it is preferable that the deciphering section is detached from the processing apparatus, fixed to a disabled state or destroyed.

[0023] Additionally, in the processing apparatus embodying the present invention stated above, it is preferable that the processing apparatus comprises ciphering pattern change means for changing a ciphering pattern whenever a predetermined initialization operation is carried out for one of the plurality of regions divided from the address space allotted to the entirety of the at least one external device.

[0024] By resetting the ciphering pattern in a predetermined initialization operation, e.g., when the processing apparatus is powered on or reset and the like, illicit interpretation is made more difficult and security thereby enhances.

[0025] Also, in the processing apparatus embodying the present invention stated above, it is preferable that the ciphering section adopts a ciphering pattern in which ciphered data is changed according to the address, for one of the plurality of regions divided from the address space allotted to the entirety of the at least one external device, to thereby cipher the data.

[0026] By adopting the function of addresses as a ciphering function to cipher the data, complicated ciphering is made possible, illicit interpretation is made more difficult and data security thereby enhances.

[0027] According to a second aspect of the present invention, there is provided an integrated circuit including a processing apparatus in accordance with the first aspect of the present invention.

[0028] An integrated circuit embodying the present invention has the above constitution and exhibits the same function and advantage as those of the processing apparatus embodying the present invention. In addition, the integrated circuit makes it difficult to interpret the circuit arrangement and the like. In this respect, too, the integrated circuit contributes to enhancing security.

[0029] Reference will now be made, by way of example, to the accompanying drawings, in which:

Fig. 1 is a block diagram of the first embodiment of a processing apparatus according to the present invention;

Fig. 2 shows a memory map of the processing apparatus shown in Fig. 1; and

Fig. 3 is a flow chart of an initialization program executed when the processing apparatus shown in Fig. 1 is powered on.

[0030] The embodiments of the present invention will be described hereinafter.

[0031] Fig. 1 is a block diagram showing an embodiment of a processing apparatus according to the present invention.

[0032] A processing apparatus 1 shown in Fig. 1 consists of a internal circuit 100 mounted inside of an LSI 10, an external circuit 200 provided externally of the LSI 10 and the others including oscillators 301 and 302 and the like. This LSI 10 corresponds to one embodiment of an integrated circuit of the present invention.

[0033] The internal circuit 100 provided within the LSI 10 has a central processing unit (CPU) 101 as well as an internal memory 102, a ciphering information register

103, an address decoder 104 and a peripheral circuit 105 which are internal devices according to the present invention. The CPU 101 and the various internal devices are mutually connected through a bus line 110. This bus line consists of an address bus 111 and a data bus 112 and extends externally of the LSI 10. Various external devices are connected to a portion 110a of the bus line 110 which extends externally. The external devices will be described later.

[0034] The internal circuit 100 constituted within the LSI 10 is provided with a ciphering section 120 interposed at an entrance to an external side. This ciphering section 120 consists of a ciphering circuit 121, a bus interface 122 and a random number generation circuit 123.

[0035] A clock signal from the oscillator 301 is inputted into the CPU 101. The CPU 101 executes various programs synchronously with the clock signal received from the oscillator 301.

[0036] A clock signal from another oscillator 302 which generates a clock signal higher in repetition frequency than the clock signal inputted into the CPU 101, is inputted into the ciphering circuit 121. The ciphering circuit 121 conducts a ciphering processing synchronously with the clock signal with a high repetition frequency from the oscillator 302. The detail of the ciphering processing will be described later.

[0037] The above two oscillators 301 and 302 generate clock signals synchronous with each other. Therefore, the oscillators 301 and 302 may generate clock signals by dividing a high-speed clock obtained by a common oscillation source.

[0038] Further, a plurality of external devices, i.e., in case of Fig. 1, a liquid crystal display (LCD) 201, a keyboard (KB) 202, a read-only memory (ROM) 203, a flash ROM 211 and a random-access memory (RAM) 212, are connected to the externally extending portion 110a of the bus line 110. In Fig. 1, a device 213 , such as another LSI , which is the same in constitution as the LSI 10 shown in Fig. 1 and which has the same ciphering mechanism as that of the internal circuit 100, and a deciphering circuit 214 for debugging programs operated by the CPU 101 are also connected to the externally extending portion 110a. The device 213 and the deciphering circuit 214 are shown in Fig. 1 for description purposes. The device 213 is connected to the LSI 10 if cipher communication is established between the LSI 10 and the device 213 having a similar constitution to that of the LSI 10. The deciphering circuit 214 is connected for program debugging and detached after the completion of debugging.

[0039] The LCD 201 and the KB 202 as well as, in case of the embodiment shown in Fig. 1. the ROM 203 belong to external devices which cipher neither addresses nor data. The flash ROM 211 and the RAM, by contrast, belong to external devices which cipher and access addresses or data. Here, the flash ROM 211 ciphers only data and the RAM ciphers both addresses and data. Further, the device 213 ciphers both addresses and data and establishes cipher communication with the LSI 10. When connected to the LSI 10, the deciphering circuit 214 belongs to the devices which cipher neither addresses nor data in this embodiment.

[0040] Here, the bus line 110 is divided into a portion connected to the CPU 101 (the address and data of which portion are denoted by A1 and D1. respectively), a portion put between the ciphering circuit 121 and the bus interface 122 (the address and data of which portion are denoted by A2 and D2, respectively) and the externally extending portion 110a of the LSI 10 (the address and data of which portion are denoted by A3 and D3, respectively).

[0041] Fig. 2 shows the memory map of the processing apparatus shown in Fig. 1.

[0042] A plurality of application programs are stored in the flash ROM which is one of the external devices. OS programs are stored in the internal memory which is one of the internal devices. Also, apparatus constitution information on this processing apparatus, e.g., types of external devices connected and memory capacities are recorded on the ROM which is one of the external devices.

[0043] Fig. 3 is a flow chart of an initialization program executed when the processing apparatus shown in Fig. 1 is powered on. This initialization program is stored in the internal memory 102 as one of the OS programs and executed by the CPU 101 when power is turned on.

[0044] According to the initialization program shown in Fig. 3, first, the apparatus constitution information stored in the ROM 203 which is one of the external devices is read (in a step al), a memory map as shown in Fig. 2 is created based on the information and a ciphering pattern is determined for each area of the memory map (in a step a2). It is noted that ciphering patterns include a pattern in which neither addresses nor data are ciphered.

[0045] In this initialization program, various other initialization processings follow (in a step a3).

[0046] Description will be continued, with reference back to Fig. 1.

[0047] The CPU 101 reads and writes information using the address A1 and the data D1. The external devices are accessed using the address A3 and the data D3 irrespectively of whether it is necessary to cipher the devices or not (or it is prohibit the devices from being ciphered).

[0048] The CPU 101 writes area information on areas to be ciphered (ciphered areas) and a ciphering pattern for each ciphered area on the memory map shown in Fig. 2, in a ciphering information register 103.

[0049] The address decoder 104 inputs the address A1 and receives the area information indicating to-be-ciphered areas from the ciphering information register 103. Then, the address decoder 104 outputs chip select signals CS0 to CS6 to an access target device and outputs a ciphering control signal Crp, indicating which de-

vice is an access target and whether or not it is necessary to conduct ciphering, to the ciphering circuit 121.

[0050] The ciphering circuit 121 receives the ciphering control signal Crp from the address decoder, conducts ciphering according to the ciphered areas when it is necessary to cipher the address A1 and data D1 based on the ciphering pattern information recorded on the ciphering pattern information register 103, and outputs the address A2 and data D2. The address A2 and data D2 are outputted externally of the LSI 10 as address A3 and data D3 by way of the bus interface 123.

[0051] An external bus access signal indicating whether an external device is to be accessed is transmitted from the CPU 101 to the bus interface 122. The bus interface 122 outputs the address A2 and data D2 outputted externally from the ciphering circuit 121 as the external address A3 and data D3 when access to the external device is requested, generates a dummy address and dummy data based on the random number from the random number generation circuit 123 and outputs the dummy address and dummy data as the external address A3 and data D3 when access to the external device is not requested. This makes illicit interpretation more difficult.

[0052] The conversion of addresses and data from internally to externally has been described. As for the data D3 read from the external flash memory 211, RAM 212, ROM 203 and the like is fetched into the internal side as the data D2. If the data is ciphered data, the ciphering circuit 121 deciphers the ciphered data and transmits the data to the CPU 101 and the like as data D1 which is not ciphered.

[0053] In this embodiment, as the ciphering pattern, a ciphering pattern in which neither addresses nor data are ciphered is adopted. In addition, the following ciphering patterns are adopted:

(1) Type 1

$$A3 = A1 \text{ XOR } p1$$

$$D3 = D1 \text{ XOR } p1$$

(2) Type 2

$$A3 = A1$$

$$D3 = A1 + D1 + p1$$

(3) Type 3

[0054] The higher level and lower level of the data as a result of the operation of type 2 are replaced.

[0055] In above types, reference p1 denotes an appropriate constant obtained by, for example, random numbers;

[0056] A XOR B signifies performing an exclusive OR operation for bits corresponding to A and B, and A + B signifies an addition operation if A and B are assumed as numeric values.

[0057] As already described above with reference to Fig. 3, in the initialization operation when power is turned on, the CPU 101 reads the apparatus constitution information stored in the ROM 203 which is one of the external devices, creates a memory map as shown in Fig. 2 and determines a ciphering pattern for each ciphered area. The flash ROM 211 adopts the ciphering pattern of, for example, (2) above in which the address is not ciphered and only the data is ciphered, and the RAM 212 adopts the ciphering pattern of, for example, (1) above in which both the address and the data are ciphered.

[0058] The RAM 212 adopts the ciphering pattern of type 1 in (1) above. Therefore, if it is assumed that p1 = 0 x 5555 (0 x means that following '5555' is a hexadecimal), both the address and the data become completely different values from the original address and data as

$$A3 \text{ (0 x 5455)}$$

$$= A1 \text{ (0 x 0100) XOR } p1 \text{ (0 x 5555)}$$

$$D3 \text{ (0 x 5476)}$$

$$= D1 \text{ (0 x 0123) XOR } p1 \text{ (0 x 5555).}$$

[0059] Further, the flash ROM 211 adopts the ciphering pattern of type 2 in (2) above. Therefore, if it is assumed that p1 = 0×5555, the address has no change and the data becomes a completely different value from the original data as follows:

$$A3 \text{ (0 x 0100)} = A1 \text{ (0 x 0100)}$$

$$D3 \text{ (0 x 5778)}$$

$$= A1 \text{ (0 x 0100)} + D1 \text{ (0 x 0123)} + p1 \text{ (0 x 5555).}$$

Here, in ciphering the data, the data is a function of the address A1. Due to this, even if the data is the same, i. e., D1, the ciphered data D3 differs from the original data according to the address A1, thereby further making illicit interpretation difficult and further enhancing security.

[0060] It is noted that the above description is a calculative example of a ciphering pattern. If an address is to be ciphered, a ciphering algorithm is taken into consideration so that a ciphered address does not over-

spread the address area of the ciphering target device and does not move to the address area of a device other than the ciphering target device.

[0061] In addition, even with the same RAM 212, it is possible to change ciphering patterns for accessing the RAM 212 according to application programs executed by the CPU 101. By not only selecting a ciphering pattern according to a memory area (a to-be-accessed external device) but also changing ciphering patterns according to application programs even in the same memory area (same external device), the address and data outputted to the externally extending portion 110a of the bus line 110 are ciphered in a more complicated manner, thereby making illicit interpretation further difficult and further enhancing security.

[0062] Here, if it is assumed that the CPU 101 and the ciphering circuit 121 operate at the same clocks, the ciphering circuit 121 cannot perform a complex ciphering operation. For example, if the CPU 101 accesses an external device at one-clock intervals, the ciphering circuit 121 is required to complete its ciphering processing within one clock. In case of the type 3 ciphering processing in (3) above, for example, it requires one-clock time to perform the type 2 ciphering in (2) and it further requires one-clock time to exchange the higher level and lower level bits. Namely, it requires a total of two-clock time and it is necessary for the ciphering circuit 121 to complete the ciphering processing within one clock, then the ciphering pattern type 3 in (3) cannot be adopted.

[0063] In case of the embodiment shown in Fig. 1, the oscillator 302 which generates a higher-speed clock than that of the oscillator 301 which supplies a clock to the CPU 101, is provided and the ciphering circuit 121 operates synchronously with the higher-speed clock supplied from the oscillator 302. Thus, for example, the ciphering pattern of type 3 in (3) above or a more complicated ciphering pattern which requires a plurality of clocks can be adopted.

[0064] For example, if a clock with 10 MH_z is supplied to the CPU 101 and a clock with 100 MH_z is supplied to the ciphering circuit 121, the ciphering circuit can perform a ciphering processing using 10 clocks.

[0065] Moreover, the internal circuit 100 of the processing apparatus shown in Fig. 1 is incorporated into the LSI 10 and address and data ciphered through the ciphering circuit 121 and the bus interface 122 are outputted from the LSI 10. With the address and data as they are, it is quite difficult for the CPU 101 to execute program debugging when developing a product employing this LSI 10. In view of this, a deciphering circuit 214 is connected to the processing circuit shown in Fig. 1.

[0066] Before debugging, information on a ciphering pattern and a ciphered area having the same content as that written into the ciphered information register 103 from the CPU 101 are written into this deciphering circuit 214. In the following debugging, the deciphering circuit 214 deciphers the ciphered address and data outputted to the externally extending portion 110a of the bus line 110 based on the information on the ciphering pattern and the ciphered area written in advance, and deciphers the address to an address and data which are not ciphered. By doing so, it is possible to monitor the address and data deciphered by the deciphering circuit 214 by using, for example, a measuring instrument and to easily debug programs executed by the CPU 101.

[0067] If this deciphering circuit 214 is left undetached, the significance of ciphering the address and data with a view to making illicit interpretation difficult is lost. For that reason, the deciphering circuit 214 is constituted as a device different from the processing apparatus and detached therefrom after the completion of debugging. Alternatively, the deciphering circuit 214 may remain attached thereto to be completely disabled.

[0068] Further, as shown in Fig. 1, the device 213 having the same ciphering mechanism as that of the LSI 10 is connected. If a plurality of LSIs 10 are combined as shown in Fig. 1, it is possible to establish cipher communication among the LSIs on the substrate.

[0069] In the above-stated embodiment, the circuit incorporated into one LSI is referred to as an internal circuit and a group of devices provided externally of the LSI is referred to as an external circuit. The internal circuit is not necessarily mounted on one LSI. It is also possible, for example, that if a circuit is dispersed and mounted on a plurality of LSIs and the plurality of LSIs are packaged in one integrated circuit package or integrally molded, then the entire circuit dispersed and mounted on these plural LSIs may be referred to as an internal circuit.

Claims

1. A processing apparatus comprising:

an internal circuit (100) including a CPU (101) executing programs, at least one internal device (102-105) having a predetermined function and bus line means (110, 111, 112) connecting said CPU (101) to said internal device (102-105), extending externally and transferring an address and data; and

an external circuit (200) provided externally of an externally extending portion (110a) of said bus line means (110, 111, 112) and including at least one external device(301,302) having a predetermined function, wherein

said internal circuit (100) includes a ciphering section (120) interposed at an entrance to an external side and ciphering the address and the data on the bus line means (110, 111, 112) by ciphering patterns according to a plurality of regions divided from an address space allotted to the entirety of said at least one external device (200);

characterised in that said ciphering section (120) outputs a dummy address and dummy data to the externally extending portion (110a) of said bus line means (110, 111, 112) at timing at which said external circuit (200) is not accessed.

2. A processing apparatus according to claim 1, wherein the ciphering patterns adopted by said ciphering section include one ciphering pattern in which neither the address nor data is ciphered.

3. A processing apparatus according to claim 1, wherein said external circuit (200) includes a plurality of external devices (201, 202, 203, 211, 212); and

said ciphering section (120) performs ciphering using ciphering patterns according to said plurality of external devices (201, 202, 203, 211, 212), respectively.

4. A processing apparatus according to claim 1, wherein said CPU (101) is supplied with a clock and executes the programs synchronously with the supplied clock, and said ciphering section (120) is supplied with a clock and performs ciphering synchronously with the supplied clock; and

further comprising a clock supply section (302) for supplying a clock at a higher speed than a speed of the clock supplied to said CPU (101), to said ciphering section.

5. A processing apparatus according to claim 1, comprising:

ciphering pattern determination means for recognizing a constitution of said external circuit and determining a ciphering pattern of said ciphering section according to the constitution of said external circuit.

6. A processing apparatus according to claim 1, wherein said ciphering section ciphers the address and the data on said bus line means by ciphering patterns according to the plurality of regions divided from the address space allotted to the entirety of said no less than one external device and according to application programs executed by said CPU.

7. A processing apparatus according to claim 1, comprising:

a deciphering section connected to the externally extending portion of said bus line means, and returning the ciphered address and the data on the bus line means to an address and data which are not ciphered.

8. A processing apparatus according to claim 1, comprising:

ciphering pattern change means for changing a ciphering pattern whenever a predetermined initialisation operation is carried out for one of the plurality of regions divided from the address space allotted to the entirety of said at least one external device.

9. A processing apparatus according to claim 1, wherein said ciphering section adopts a ciphering pattern in which ciphered data is changed according to the address, for one of the plurality of regions divided from the address space allotted to the entirety of said at least one external device, to thereby cipher the data.

10. An integrated circuit including a processing apparatus as claimed in any preceding claim.

Patentansprüche

1. Verarbeitungsvorrichtung, welche umfasst:

eine interne Schaltung (100), welche eine CPU (101), die Programme ausführt, mindestens ein internes Gerät (102-105), welches eine vorbestimmte Funktion hat, und Busleitungsmittel (110, 111, 112) enthält, welche die CPU (101) mit dem internen Gerät (102-105) verbinden, sich nach außen erstrekken und eine Adresse und Daten übertragen, und

eine externe Schaltung (200), welche sich außerhalb eines sich nach außen erstreckenden Teils (110a) der Busleitungsmittel (110, 111, 112) befindet und mindestens ein externes Gerät (301, 302) enthält, das eine vorbestimmte Funktion hat, wobei

die interne schaltung (100) einen Verschlüsselungsabschnitt (120) aufweist, der an einen Eingang zu einer externen Seite zwischengeschaltet ist und die Adresse und die Daten auf den Busleitungsmitteln (110, 111, 112) verschlüsselt durch Verschlüsselung von Mustern entsprechend einer Anzahl von Bereichen, die abgetrennt sind von einem Adressenraum, welcher der aus mindestens einem Gerät bestehenden Gesamtheit der externen Geräte (200) zugeordnet ist;

dadurch gekennzeichnet, dass der Verschlüsselungsabschnitt (120) an den sich nach außen erstreckenden Teil (110a) der Busleitungsmittel (110, 111, 112) eine Scheinadresse und Scheindaten ausgibt zu Zeiten, zu denen auf die externe

Schaltung (200) nicht zugegriffen wird.

2. Verarbeitungsvorrichtung gemäß Anspruch 1, bei welcher die vom Verschlüsselungsabschnitt übernommenen Verschlüsselungsmuster ein Verschlüsselungsmuster enthalten, in welchem weder die Adresse noch die Daten verschlüsselt sind.

3. verarbeitungsvorrichtung gemäß Anspruch 1, bei welcher die externe Schaltung (200) eine Anzahl von externen Geräten (201, 202, 203, 211, 212) enthält, und

der Verschlüsselungsabschnitt (120) die Verschlüsselung ausführt unter Verwendung von Verschlüsselungsmustern entsprechend der Anzahl der jeweiligen externen Geräte (201, 202, 203, 211, 212).

4. Verarbeitungsvorrichtung gemäß Anspruch 1, bei welcher die CPU (101) einen Takt zugeführt bekommt und die programme synchron mit diesem zugeführten Takt ausführt und der Verschlüsselungsabschnitt (120) einen Takt zugeführt bekommt und die Verschlüsselung synchron mit diesem zugeführten Takt ausführt, und

welche ferner einen Taktgeberbereich (302) umfasst, damit dem Verschlüsselungsabschnitt ein Takt mit einer höheren Geschwindigkeit als der Geschwindigkeit des der CPU (101) zugeführten Taktes zugeführt wird.

5. Verarbeitungsvorrichtung gemäß Anspruch 1, welche umfasst:

Verschlüsselungsmuster-Änderungsmittel, um die Struktur der externen Schaltung zu erkennen und ein Verschlüsselungsmuster des Verschlüsselungsabschnitts entsprechend der Struktur der externen Schaltung zu bestimmen.

6. Verarbeitungsvorrichtung gemäß Anspruch 1, bei welcher der Verschlüsselungsabschnitt die Adresse und die Daten auf den Busleitungsmitteln verschlüsselt durch verschlüsselung von Mustern entsprechend der Anzahl der Bereiche, die von dem Adressenraum abgetrennt sind, welcher der aus mindestens einem Gerät bestehenden Gesamtheit der Geräte zugeordnet ist, und entsprechend den von der CPU ausgeführten Anwendungsprogrammen.

7. Verarbeitungsvorrichtung gemäß Anspruch 1, welche umfasst:

einen Entschlüsselungsabschnitt, welcher an den sich nach außen erstreckenden Teil der Busleitungsmittel angeschlossen ist und die verschlüsselte Adresse und die Daten auf den Busleitungsmitteln in eine Adresse und in Daten, die unverschlüsselt sind, rückführt.

8. Verarbeitungsvorrichtung gemäß Anspruch 1, welche umfasst:

Verschlüsselungsmister-Änderungsmittel zum Ändern eines Verschlüsselungsmusters immer dann, wenn eine vorbestimmte Initialisierungsoperation für einen Bereich aus der Anzahl von Bereichen ausgeführt wird, die von dem Adressenraum abgetrennt sind, welcher der Gesamtheit aus mindestens einem externen Gerät zugeordnet ist.

9. Verarbeitungsvorrichtung gemäß Anspruch 1, bei welcher der Verschlüsselungsabschnitt ein Verschlüsselungsmuster übernimmt, in welchem verschlüsselte Daten entsprechend der Adresse geändert werden für einen Bereich aus der Anzahl von Bereichen, die von dem Adressenraum abgetrennt sind, welcher der Gesamtheit aus mindestens einem externen Gerät zugeordnet ist, um dadurch die Daten zu verschlüsseln.

10. Integrierter Schaltkreis, welcher eine Verarbeitungsvorrichtung enthält, wie sie in irgend einem der vorangehenden Ansprüche beansprucht ist.

Revendications

1. Dispositif de traitement comportant :

un circuit interne (100) comprenant une CPU (101) exécutant des programmes, au moins un dispositif interne (102-105) possédant une fonction prédéterminée et des moyens de ligne de bus (110, 111, 112) reliant ladite CPU (101) audit dispositif interne (102-105), s'étendant extérieurement et transférant une adresse et des données ; et
un circuit externe (200) prévu à l'extérieur d'une partie s'étendant extérieurement (110a) desdits moyens de ligne de bus (110, 111, 112) et comprenant au moins un dispositif externe (301, 302) possédant une fonction prédéterminée, dans lequel
ledit circuit interne (100) comprend une section de chiffrement (120) interposée à une entrée au côté externe et chiffrant l'adresse et les données sur les moyens de ligne de bus (110, 111, 112) en chiffrant des modèles selon une pluralité de régions séparées d'un espace d'adresse alloué à la totalité dudit au moins un dispositif externe (200) ;

caractérisé en ce que ladite section de chif-

frement (120) délivre une adresse fictive et des données fictives à la partie s'étendant extérieurement (110a) desdits moyens de ligne de bus (110, 111, 112) à un moment auquel ledit circuit externe (200) n'est pas accédé.

2. Dispositif de traitement selon la revendication 1, dans lequel les modèles de chiffrement adoptés par ladite section de chiffrement comprennent un modèle de chiffrement dans lequel ni l'adresse ni les données ne sont chiffrées.

3. Dispositif de traitement selon la revendication 1, dans lequel ledit circuit externe (200) comprend une pluralité de dispositifs externes (201, 202, 203, 211, 212); et

ladite section de chiffrement (120) effectue un chiffrement en utilisant des modèles de chiffrement selon ladite pluralité de dispositifs externes (201, 202, 203, 211, 212), respectivement.

4. Dispositif de traitement selon la revendication 1, dans lequel ladite CPU (101) est équipée d'une horloge et exécute les programmes de façon synchrone avec l'horloge fournie, et ladite section de chiffrement (120) est équipée d'une horloge et effectue un chiffrement de façon synchrone avec l'horloge fournie ; et

comportant en outre une section d'alimentation d'horloge (302) pour alimenter une horloge à une vitesse plus élevée qu'une vitesse de l'horloge délivrée à ladite CPU (101), à ladite section de chiffrement.

5. Dispositif de traitement selon la revendication 1, comportant :

des moyens de détermination de modèle de chiffrement pour reconnaître un agencement dudit circuit externe et pour déterminer un modèle de chiffrement de ladite section de chiffrement selon l'agencement dudit circuit externe.

6. Dispositif de traitement selon la revendication 1, dans lequel ladite section de chiffrement chiffre l'adresse et les données sur lesdits moyens de ligne de bus en chiffrant des modèles selon la pluralité de régions séparées d'un espace d'adresse alloué à la totalité dudit pas moins d'un dispositif externe et selon les programmes d'application exécutés par ladite CPU.

7. Dispositif de traitement selon la revendication 1, comportant :

une section de décodage reliée à la partie s'étendant extérieurement desdits moyens de ligne de bus, et en retournant l'adresse et les données chiffrées sur les moyens de ligne de bus à l'adresse et aux données qui ne sont pas chiffrées.

8. Dispositif de traitement selon la revendication 1, comportant :

des moyens de changement de modèle de chiffrement pour changer un modèle de chiffrement chaque fois qu'une opération d'initialisation prédéterminée est mise en oeuvre pour l'une de la pluralité de régions séparées d'un espace d'adresse alloué à la totalité dudit au moins un dispositif externe.

9. Dispositif de traitement selon la revendication 1, dans lequel ladite section de chiffrement adopte un modèle de chiffrement dans lequel les données chiffrées sont changées selon l'adresse, pour l'une de la pluralité de régions séparées d'un espace d'adresse alloué à la totalité dudit au moins un dispositif externe, pour ainsi chiffrer les données.

10. Circuit intégré comprenant un dispositif de traitement selon l'une quelconque des revendications précédentes.

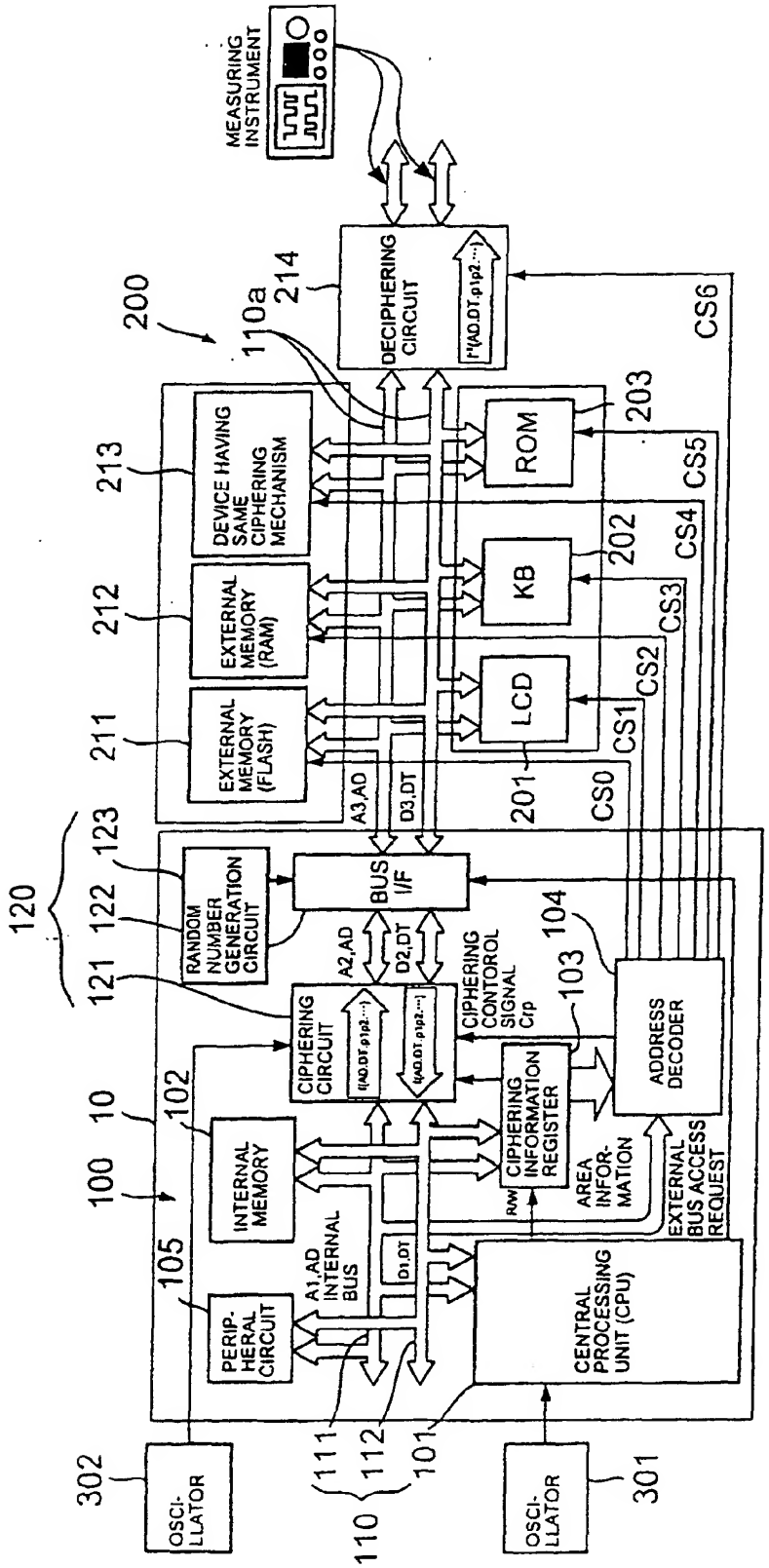
MEASURING INSTRUMENT
200
110a
214
DECIPHERING CIRCUIT
CS6
203
ROM
CS5
213
DEVICE HAVING SAME CIPHERING MECHANISM
202
KB
CS4
212
EXTERNAL MEMORY (RAM)
CS3
CS2
211
EXTERNAL MEMORY (FLASH)
LCD
CS1
CS0
201
A3,AD
D3,DT
123
120
122
RANDOM NUMBER GENERATION CIRCUIT
BUS I/F
121
A2,AD
D2,DT
104
CIPHERING CONTOROL SIGNAL Crp
103
CIPHERING CIRCUIT
ADDRESS DECODER
102
10
100
INTERNAL MEMORY
CIPHERING INFORMATION REGISTER
R/W
AREA INFOR-MATION
EXTERNAL BUS ACCESS REQUEST
105
A1,AD INTERNAL BUS
D1,DT
PERIP-HERAL CIRCUIT
CENTRAL PROCESSING UNIT (CPU)
302
OSCI-LLATOR
111
112
110
101
OSCI-LLATOR
301

Fig. 1

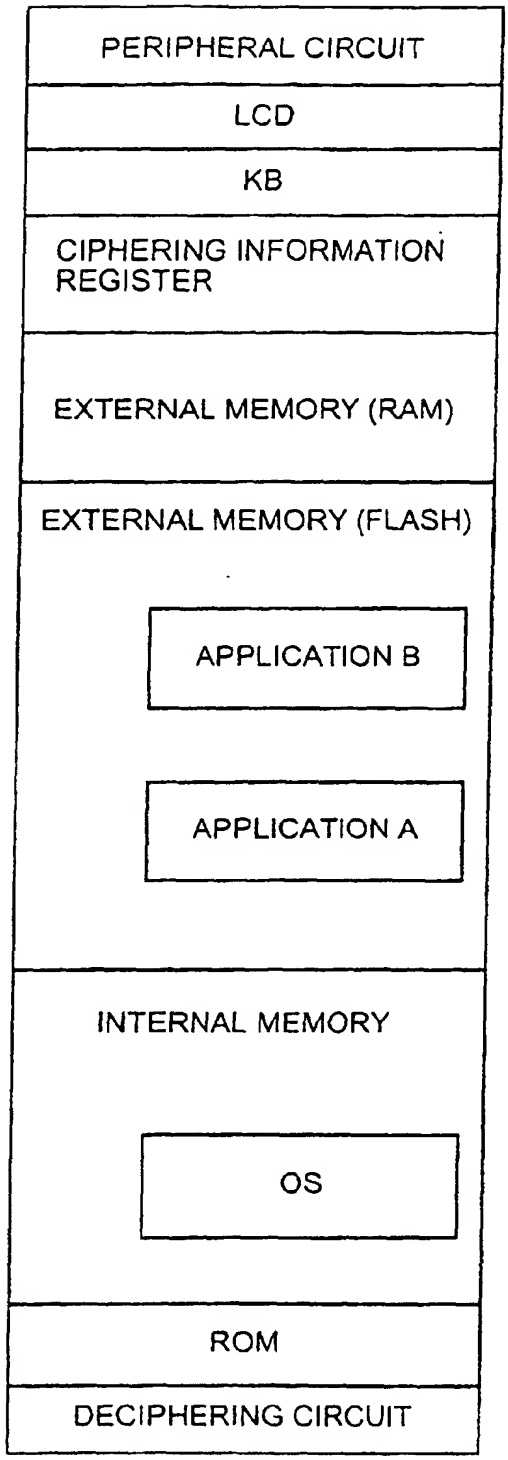
PERIPHERAL CIRCUIT
LCD
KB
CIPHERING INFORMATION REGISTER
EXTERNAL MEMORY (RAM)
EXTERNAL MEMORY (FLASH)
APPLICATION B
APPLICATION A
INTERNAL MEMORY
OS
ROM
DECIPHERING CIRCUIT

Fig. 2

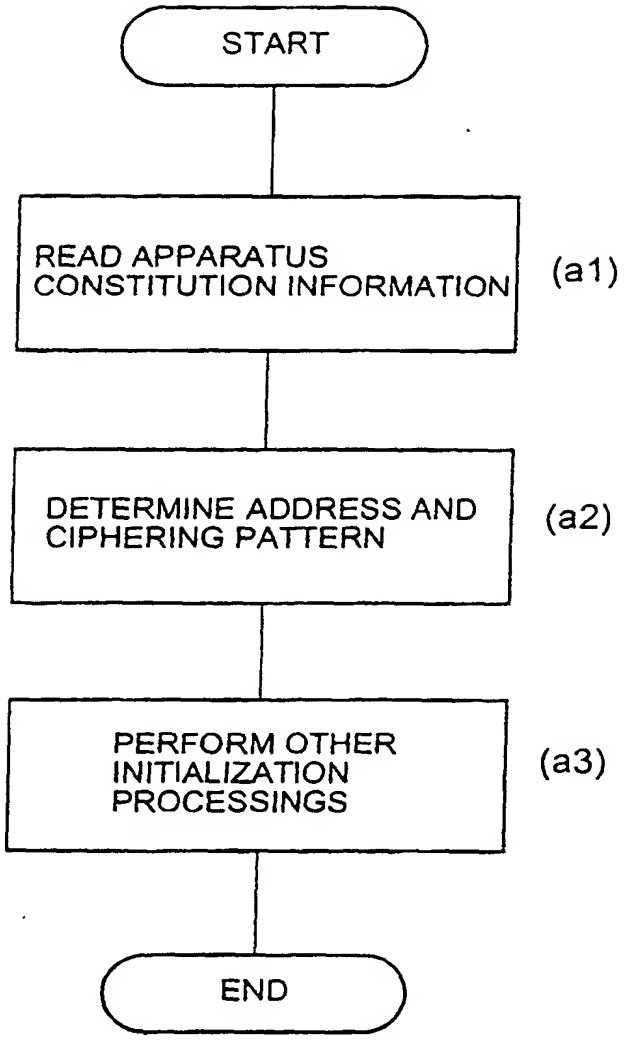
START
READ APPARATUS CONSTITUTION INFORMATION
(a1)
DETERMINE ADDRESS AND CIPHERING PATTERN
(a2)
PERFORM OTHER INITIALIZATION PROCESSINGS
(a3)
END

Fig. 3